History of the BCA concept and other BCA efforts

Robert Moskowitz

rgm@icsa.net
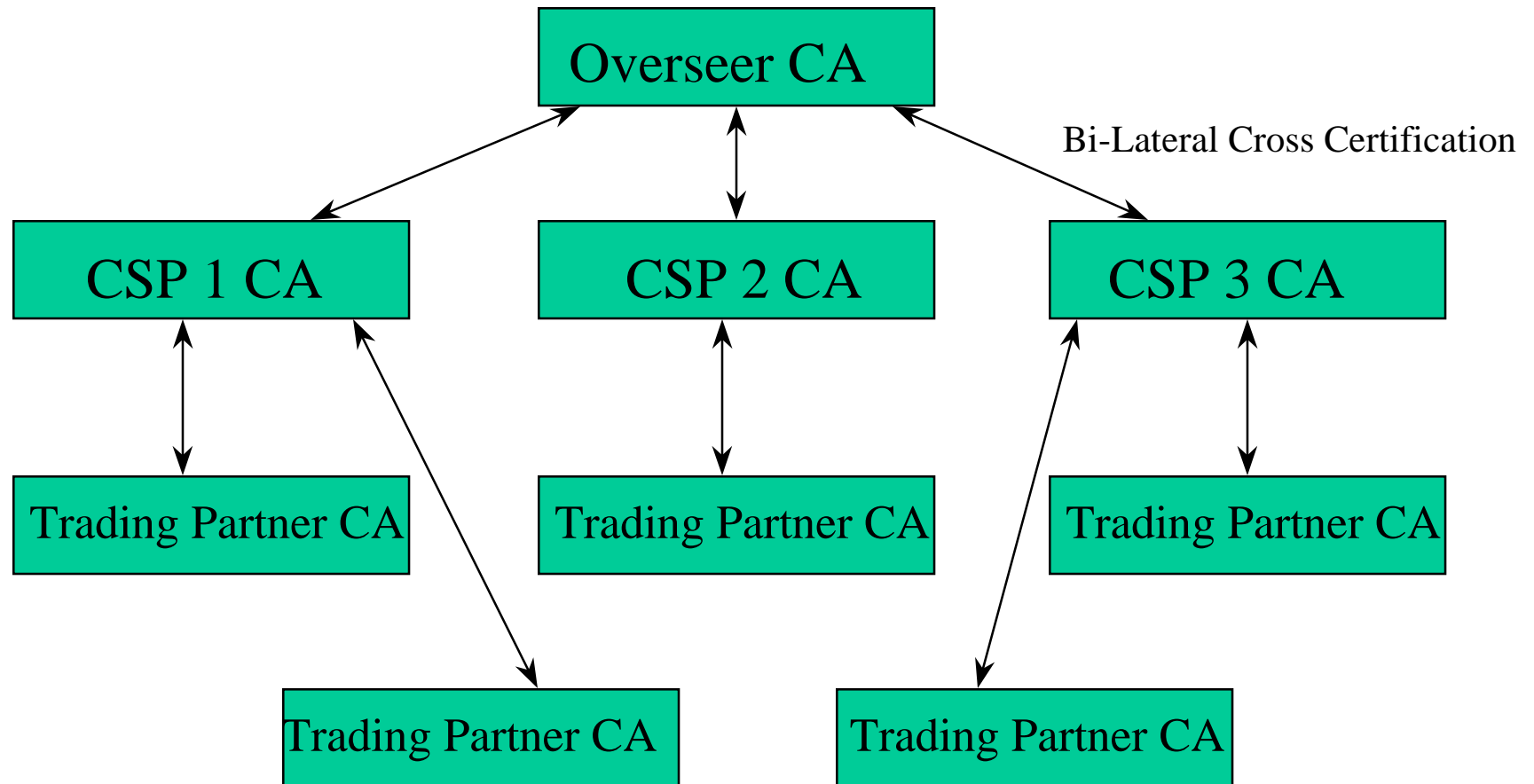
Apr 5, 2000

ICSA.net

WE SECURE THE WEB

Trust in a Community Of Interest

- Entrance MUST be easy in a COI
- Dismissal MUST be fast and effective in a COI
- No one is guaranteed a role in a COI
- Liability is defined by the COI

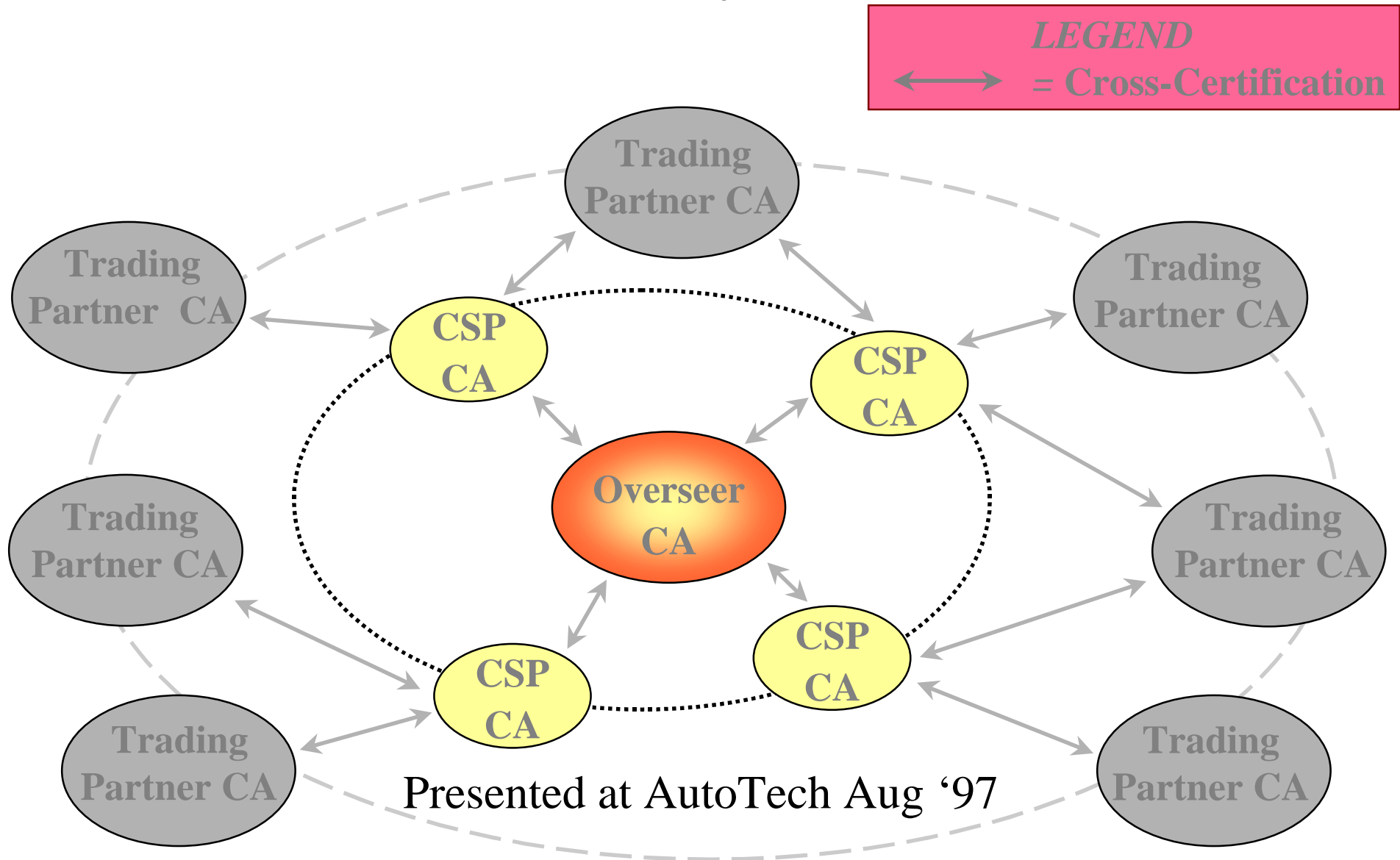# ANX Public Key Infrastructure

Overseer CA

Bi-Lateral Cross Certification

CSP 1 CA

CSP 2 CA

CSP 3 CA

Trading Partner CA

Trading Partner CA

Trading Partner CA

Trading Partner CA

Trading Partner CA

Presented at Bellcore Security Conference Apr '97

Building Trust in a COI

- Growth must be 'Organic'
  - Any part MAY come first
  - Infrastructure developed as needed
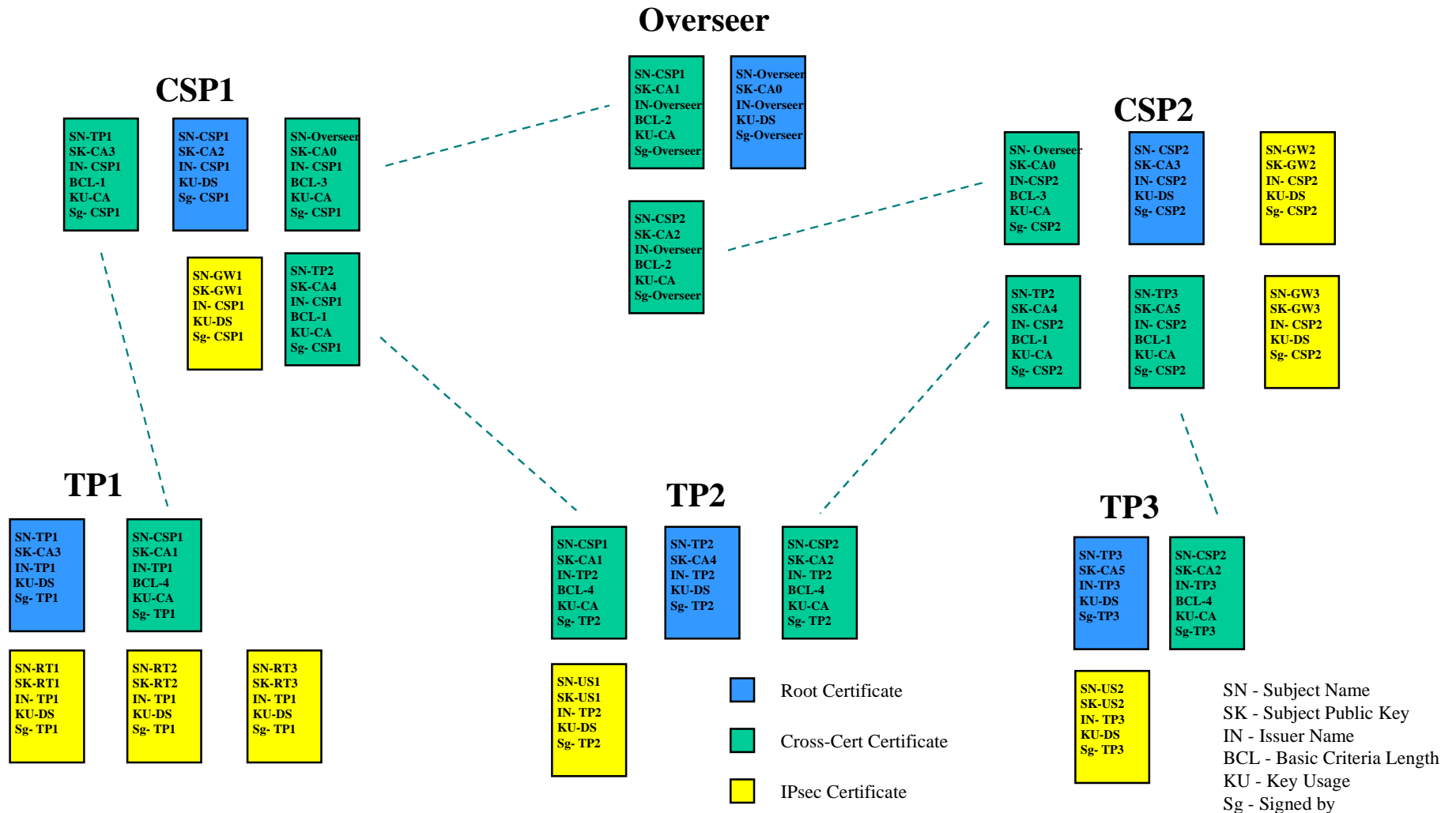- Late-comers not penalized
- COI controls its destiny

Bridging Trust in a COI

- Bridging a Ring of Trust
  - Building spokes to the rings
- But can it be built?

ANX PKI

Overseer

SN-CSP1 SK-CA1 IN-Overseer BCL-2 KU-CA Sg-Overseer

SN-Overseer SK-CA0 IN-Overseer KU-DS Sg-Overseer

SN-CSP2 SK-CA2 IN-Overseer BCL-2 KU-CA Sg-Overseer

CSP1

SN-TP1 SK-CA3 IN- CSP1 BCL-1 KU-CA Sg- CSP1

SN-CSP1 SK-CA2 IN- CSP1 KU-DS Sg- CSP1

SN-Overseer SK-CA0 IN- CSP1 BCL-3 KU-CA Sg- CSP1

SN-GW1 SK-GW1 IN- CSP1 KU-DS Sg- CSP1

SN-TP2 SK-CA4 IN- CSP1 BCL-1 KU-CA Sg- CSP1

CSP2

SN- Overseer SK-CA0 IN-CSP2 BCL-3 KU-CA Sg- CSP2

SN- CSP2 SK-CA3 IN- CSP2 KU-DS Sg- CSP2

SN-GW2 SK-GW2 IN- CSP2 KU-DS Sg- CSP2

SN-CSP2 SK-CA2 IN-Overseer BCL-2 KU-CA Sg-Overseer

SN-TP2 SK-CA4 IN- CSP2 BCL-1 KU-CA Sg- CSP2

SN-TP3 SK-CA5 IN- CSP2 BCL-1 KU-CA Sg- CSP2

SN-GW3 SK-GW3 IN- CSP2 KU-DS Sg- CSP2

TP1

SN-TP1 SK-CA3 IN-TP1 KU-DS Sg- TP1

SN-CSP1 SK-CA1 IN-TP1 BCL-4 KU-CA Sg- TP1

SN-RT1 SK-RT1 IN- TP1 KU-DS Sg- TP1

SN-RT2 SK-RT2 IN- TP1 KU-DS Sg- TP1

SN-RT3 SK-RT3 IN- TP1 KU-DS Sg- TP1

TP2

SN-CSP1 SK-CA1 IN-TP2 BCL-4 KU-CA Sg- TP2

SN-TP2 SK-CA4 IN- TP2 KU-DS Sg- TP2

SN-CSP2 SK-CA2 IN- TP2 BCL-4 KU-CA Sg- TP2

SN-US1 SK-US1 IN- TP2 KU-DS Sg- TP2

TP3

SN-TP3 SK-CA5 IN-TP3 KU-DS Sg-TP3

SN-CSP2 SK-CA2 IN-TP3 BCL-4 KU-CA Sg-TP3

SN-US2 SK-US2 IN- TP3 KU-DS Sg- TP3

- ■ (blue) Root Certificate
- ■ (green) Cross-Cert Certificate
- ■ (yellow) IPsec Certificate

SN - Subject Name
SK - Subject Public Key
IN - Issuer Name
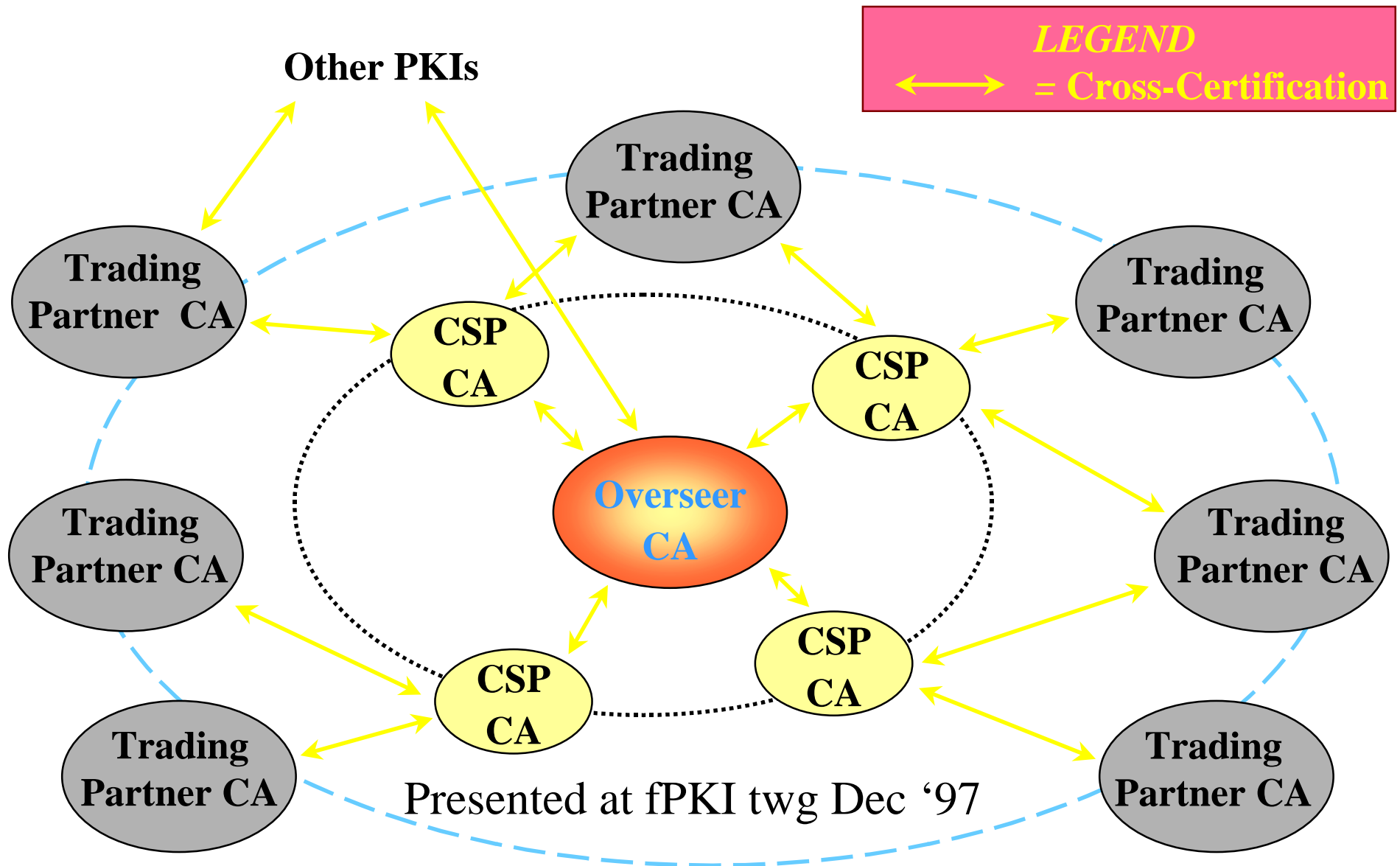BCL - Basic Criteria Length
KU - Key Usage
Sg - Signed by

Bridging Trust in a COI

- The CONCEPT fits the technology
  - Maturation along operational considerations
    - No EE certificates from Bridging or 'Infrastructure' CAs
- The CONCEPT fits operational realities
- Can we sell it and deploy it

Expanding the Bridges

- Trust between bridges
- Bridges of Bridges?

What is happening

- Federal PKI adopted the Bridge model in Feb '98
  - Into Pilot
- ANX floundered on application readiness
  - Put off for Ecommerce future (2001)
- California Medical Community
  - Pilot this year
- FannieMae - concept
- Internet2 - Direction